Virtual Private Network (VPN)

What is a VPN?

A ***virtual private network (VPN)*** is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

- Remote network communication through Internet
- Became popular as more employees worked in remote locations.
- In order to gain access to the private network, a user must be authenticated using a unique identification and a password.
- Used by companies/organizations who want to communicate confidentially
- The Internet is used as the backbone for VPNs

Brief Overview of How it Works

Two connections – one is made to the Internet and the second is made to the VPN.

Datagram's – contains data, destination and source information.

Firewalls – VPNs allow authorized users to pass through the firewalls.

Protocols – protocols create the VPN tunnels.

Four Critical Functions

Authentication – validates that the data that sent from the sender.

Access control – limiting unauthorized users from accessing the network.

Confidentiality – preventing the data to be read or copied as the data is being transported.

Data Integrity – ensuring that the data has not been altered.

Types of VPN

3 Types

- Remote Access – Employee to Business
- Intranet – Within an organization
- Extranet – Outside an organization

Remote-access-is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.

A good example of a company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field.

Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

Intranet-based - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

Extranet-based - When a company has a close relationship with *another company* (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

VPN Protocols

` The number of protocols and available security features continue to grow with time. The most common protocols are:

Point-to-point tunneling protocol (PPTP)

- PPTP has been around since the days of Windows 95.
- It can be *easily setup on every major OS*.
- It is still strong, but not the most secure.

L2TP/IPSec (Layer Two tunneling protocol /Internet Protocol Security)

- L2TP over IPSec is *more secure* than PPTP and offers more features. L2TP/IPsec is a way of implementing two protocols together in order to gain the best features of each.

Open VPN - The software used is *open source* and *freely available*. OpenVPN can run on a single UDP or TCP port, making it *extremely flexible*.

	STANDARD VPN PPTP	STANDARD VPN L2TP/IPsec	SECURE VPN OpenVPN
Level encryption	128 BIT	128 BIT	256 BIT
Supported OS	• Windows • Mac OS X • Linux • iOS • Android • Windows Phone • DD-WRT	• Windows • Mac OS X • Linux • iOS • Android • Windows Phone • DD-WRT	• Windows • Mac OS X • Linux • iOS • Android
Compatibility	Desktops, laptops, tablets, smartphones.	Desktops, laptops, tablets, smartphones.	Desktops, Notebooks.
Security	Basic encryption up to 128bit.	Strong encryption. In addition, the data wraps IPsec up to 128bit.	Very strong encryption using certificates up to 256bit
Speed	A very fast due to the basic encryption	Requires more CPU to encrypt data	Best performance. Very fast, even on connection with high delay

Configuration	Very simple. The protocol built into most devices. Does not require additional software	Simple, requires additional settings. The protocol built into most devices. Does not require additional software	Additional software required. Need to install certificates
Used ports	• TCP 1723 • GRE	• UDP 1701 • UDP 500 • UDP 4500 • ESP	• TCP 993 • TCP 443
Summary	PPTP is fast and very easy to set up. It is a good choice if your device does not support OpenVPN or SSTP VPN. Recommended for mobile devices.	L2TP/IPsec is a good choice if your device does not support OpenVPN or SSTP VPN and you care about the high security. Recommended for mobile devices.	OpenVPN is the recommended protocol for Windows, Linux and Mac OS X. The highest performance, security and reliability.

VPN: Advantages

- Cost Effective
- Greater scalability
- Easy to add/remove users
- Mobility
- Security

VPN: Disadvantages

- Understanding of security issues
- Unpredictable Internet traffic
- Difficult to accommodate products from different vendors

Industries That May Use a VPN

Healthcare: enables the transferring of confidential patient information within the medical facilities & health care provider

Manufacturing: allow suppliers to view inventory & allow clients to purchase online safely

Retail: able to securely transfer sales data or customer info between stores & the headquarters

Banking/Financial: enables account information to be transferred safely within departments & branches

General Business: communication between remote employees can be securely exchanged

Thank you